



CVE-2020-8261

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-8261
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-28 13:15:00 UTC
Updated	2024-01-13 04:43:00 UTC
Description	A vulnerability in the Pulse Connect Secure / Pulse Policy Secure < 9.1R9 is vulnerable to arbitrary cookie injection.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ivanti	Policy Secure	9.1	r1	All	All
Application	Ivanti	Policy Secure	9.1	r2	All	All
Application	Ivanti	Policy Secure	9.1	r3	All	All
Application	Ivanti	Policy Secure	9.1	r4	All	All
Application	Ivanti	Policy Secure	9.1	r5	All	All
Application	Ivanti	Policy Secure	9.1	r6	All	All
Application	Ivanti	Policy Secure	9.1	r7	All	All
Application	Ivanti	Policy Secure	9.1	r8	All	All
Application	Pulsesecure	Pulse Connect Secure	All	All	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r1	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r2	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r3	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r4	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r5	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r6	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r7	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r8	All	All

Application	Pulsesecure	Pulse Connect Secure	All	All	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r1	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r2	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r3	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r4	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r5	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r6	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r7	All	All
Application	Pulsesecure	Pulse Connect Secure	9.1	r8	All	All
Application	Pulsesecure	Pulse Policy Secure	All	All	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r1	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r2	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r3	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r4	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r5	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r6	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r7	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r8	All	All
Application	Pulsesecure	Pulse Policy Secure	All	All	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r1	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r2	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r3	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r4	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r5	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r6	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r7	All	All
Application	Pulsesecure	Pulse Policy Secure	9.1	r8	All	All

References

Reference

Public KB - SA44601 - 2020-10: Security Bulletin: Multiple Vulnerabilities Resolved in Pulse Connect Secure / Pulse Policy Secure / Pulse Sec

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)